Personnel Cabinet (PC) – Division of Technology Services (DTS)
Information Technology (IT) Policies

Category: 010.000 Logical Security

010.102 Application Access Control

Policy: Procedures for Controlling Personnel Cabinet Data/Information Access.

Scope: This policy applies to all PC employees, Enterprise HR Users and contractors, including all persons who provide contract services, use, process, or store data relevant to agency business.

Policy/Procedure Maintenance Responsibility: DTS Access Control Branch is responsible for the maintenance of this policy.

Applicability: All users who access Personnel Cabinet and/or data. This procedure also includes vendors and / or contractors who access Personnel Cabinet data.

Exceptions: Any exceptions to this policy must follow the procedures established in PC-DTS IT Policy #060.101.

Description of Components: Details the Personnel Cabinet human resource data access procedures. Planning and provision for access will be provided by the Personnel Cabinet, Access Control Branch located within the Department of Human Resources Administration, Division of Technology Services. The Personnel Cabinet adheres to policies, standards and procedures to protect information from unauthorized, accidental, intentional or malicious modification, destruction or disclosure. The Personnel Cabinet implements internal policies and standards and follows the Commonwealth Office of Technology's Enterprise Standards. Modifications to this document must have the approval of the Personnel Cabinet Change Control Committee (CCC).

Procedures:
The Personnel Cabinet in partnership with agencies and other entities ensures that access control provisions and safeguards are in place for authorized users. The following outlines this process:

- A Memorandum of Agreement (MOA) relating to accessing and use of Personnel Cabinet data information shall be signed by the Agency's Cabinet Secretary or Agency Head and the Commissioner of the Department of Human Resources Administration. The MOA encompasses all Personnel Cabinet Data Systems.
- The Agency Head/Designee shall designate a member(s) of the Agency's Human Resources Administration Staff as an Agency Security Contact(s) on the Agency Security Contact(s) Designation/Removal Form.
    - If the Agency Head/Designee ***is*** the Agency Security Contact (i.e.: Boards and Commissions) and therefore ***must*** request their own access and/or increase in authority; they must complete an Exception Request letter to the Director of the Division of Employee Management for approval.
    - If the Agency Head/Designee cannot designate a member of the Agency's Human

Resources Administration Staff as an Agency Security Contact a designee of the Commissioner's Office of the Department of Human Resources Administration may act as Agency Security Contact for that Agency.
    - The Agency Security Contact for all Agency users of the KEHP program is a designee of the Commissioner's Office of the Department of Employee Insurance.
- All designated Agency Security Contacts are required to sign an Agency Security Contact Agreement which outlines their responsibilities and allows them to request access to any Personnel Cabinet Human Resource system for users in their agency.
- Designated Agency Security Contacts are responsible for requesting access for specific staff to Personnel Cabinet systems; additional access, changes to existing access, and/or to revoke access.
- Designated Agency Security Contacts shall inform users that the KHRIS ESS/MSS online User Agreement Form applies to ALL Personnel Cabinet systems and access granted within each system. The online KHRIS User Agreement form will be presented to all users upon initial access to KHRIS and must be updated online yearly to remain an active user of all Personnel Cabinet systems to which access is granted.
- Elevated access to Personnel Cabinet systems requires acknowledgement of review of all information in the Information, Security, Training, Education, Policies/Procedures (iSTEP) Portal which is tailored based on user group. Agency Security Contacts are required to ensure this review as well as any role-specific training requirements are met prior to submitting a request for a user's access.
- Any missing information, incorrect access levels or any other item not accurately reflected on the Personnel Cabinet Systems Request Form will result in the Form being returned for correction.
- Any access request outside of the Agency's org group must provide justification and must be approved by the Director of the Division of Employee Management and/or the Commissioner of the Department of Human Resources Administration.

Designated Agency Security Contacts and the Personnel Cabinet Access Control Branch will ensure access to Personnel Cabinet systems/data is current. The Kentucky Human Resource Information System's (KHRIS) security is position based. The Agency Security Contacts will review the following circumstances to request appropriate modification and/or revocation of access privileges if/when not controlled by the system itself:

- When users transfer in or out of current position type; modify or revoke privileges;
- During a user's extended leave, and/or when deemed appropriate by Agency Security Contact, revoke access privileges; and
- Termination of user from the Commonwealth, revoke all access privileges.

Additionally, any KHRIS roles that require Personnel Cabinet sponsored training will be programmatically delimited from vacated positions. Security in other Personnel Cabinet systems is not position based like in KHRIS so the analysis of the circumstances above is even more critical when reviewing users' access to other Personnel Cabinet systems.

No one may submit a Personnel Cabinet Systems Request Form requesting access or an increase in authority for themselves for their User ID. For example, if the request is for a designated Agency Security Contact, then an Agency Head/Designee or an alternate Agency Security

Contact within the agency will need to submit the form through the HR portal.

- The only exception to this rule is if an exception request, previously sent to the Director of the Division of Employee Management or above, was approved.

Access to a Personnel Cabinet system may be provided upon electronic receipt of the Personnel Cabinet Systems Request Form. This electronic copy will serve as the official record. When required, the Personnel Cabinet will provide new users their login credentials via email. Upon the first login, the new user will be prompted by the system to change their password. The user's password must adhere to standards for each system. The Personnel Cabinet's Access Control Branch will process the request from the Agencies in a timely manner. Other security settings and procedures will be addressed for each system. Wherever possible, these will be standardized.

Timeline:
Revision date:
Review date:
Effective date: 05/19/2016